NAVAL WAR COLLEGE
Newport, R.I.

Port and Rail Vulnerabilities in the Age of Information Warfare

by

Elaine A. Therianos
GS-13 CIA

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College of the Department of the Navy.

Signature _____

8 February 2000

Advisor _____
Captain Scott Thompson, USN

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT	
6. Office Symbol: C	**7. Address:** NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Port and Rail Vulnerabilities in Information Warfare (U)	
9. Personal Authors: Elaine Therianos, CIV	
10. Type of Report: FINAL	**11. Date of Report:** 8 February 2000
12. Page Count: 21	**12A Paper Advisor (if any): Captain Scott Thompson**
13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: information warfare, port vulnerabilities, rail vulnerabilities, operational deployment, commercial systems, EDI, networks,	

15. Abstract: The United States military relies on military systems as well as commercial systems at rail and port facilities for rapid deployment capability. Because several of the systems that are relied upon do not have adequate security, an information warfare attack against these systems can and will deny the military the capability to deploy rapidly, severely hampering operational tempo. Information warfare attacks against US rail or port facilities could cause so much confusion and the cascading effects could run so deep, that the US could reach culmination prior to even leaving the shore. It is vital that the US make commercial entities aware of the vulnerabilities, and help to protect those systems where ever possible. Finally, just as the US deterred nuclear warfare by stating that the consequences of such an act would be more costly to the attacker, so must the US deter the information warfare attacker by assuring that punishment will be swift, just and costly. The US military cannot afford to have deployment capabilities disrupted, delayed or denied. As the only super power left in the world, the US must be capable of power projection to protect US national interests abroad.

16. Distribution / Availability of Abstract:	**Unclassified**	**Same As Rpt**	**DTIC Users**
	X		

17. Abstract Security Classification: UNCLASSIFIED	
18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT	
19. Telephone: 841-6461	**20. Office Symbol:** C

Security Classification of This Page Unclassified

Abstract of

PORT AND RAIL VULNERABILITIES IN THE AGE OF INFORMATION WARFARE

The United States military relies on military systems as well as commercial systems at rail and port facilities for rapid deployment capability. Because several of the systems that are relied upon do not have adequate security, an information warfare attack against these systems can and will deny the military the capability to deploy rapidly, severely hampering operational tempo. Information warfare attacks against US rail or port facilities could cause so much confusion and the cascading effects could run so deep, that the US could reach culmination prior to even leaving the shore. It is vital that the US make commercial entities aware of the vulnerabilities, and help to protect those systems where ever possible. Finally, just as the US deterred nuclear warfare by stating that the consequences of such an act would be more costly to the attacker, so must the US deter the information warfare attacker by assuring that punishment will be swift, just and costly. The US military cannot afford to have deployment capabilities disrupted, delayed or denied. As the only super power left in the world, the US must be capable of power projection to protect US national interests abroad.

Everywhere, computers and other digital devices have insinuated themselves into our lives. What was manual is now automated; what was analog is now digital; and what once stood alone is now connected to everything else. Increasingly, we have no choice but to trust them. If they fail, we are sunk.[1]

Martin Libicki

Introduction

The post-Cold War Years saw the closing of US bases overseas in order to save already scarce Defense dollars. As a result, power projection has become vital to US national interests. Military deployments from the US responding to crises overseas are more prevalent and will become more challenging in the coming years. Deployments from within the US will require the use of civilian run rail lines and port facilities, and their associated networks to ensure mobilization, deployment, and sustainment progress in a timely manner. George Tenet, the Director of Central Intelligence, outlines the vulnerabilities of civilian as well as military networks, and how Information Warfare attacks could bring the "fog of war" to the United States.

"Through high-tech attacks, "Information Warfare" would exploit growing reliance on the bits and bytes that weave modern societies together for everything from telecommunications to power grids, banking, and transportation. It is clear that nations developing these programs recognize the value of attacking a country's computer systems both on the battlefield and in the civilian arena."[2]

By taking control of these key systems, computer attackers could prevent the US military from responding to crises abroad quickly.

Deployment of the US military overseas relies heavily on the US civil sector and is increasingly becoming dependent on elements of the National Information

---

[1] Martin Libicki,. "Ghosts in the Machines?" USIA Washington File, 4 Novemeber 1998, http://www.fas.org/irp/news/1998/11/98110403_plt.html (22 January 2000). 1

[2] George Tenent, "China, others spot U.S. computer weaknesses: CIA," http://www/freerepublic.com (20 January 2000). 1

Infrastructure.[3] This, in turn is giving rise to the growth of a Transportation Information Infrastructure, and the Intelligent Transportation Systems (ITS).[4] A large mobilization and deployment effort will require the uninterrupted flow of information for command and control. Port and rail facilities that will be participating in conducting deployment operations are relying on ITS, Geographic Information Systems (GIS), and Global Positioning Systems (GPS) for the provision of real-time information on infrastructure and service performance, tracking shipments, and ensuring responsive, efficient, safe and reliable transport.[5]

While information and communications technologies can significantly enhance the performance of transportation functions technologies can also make transportation more vulnerable to loss through deliberate compromise or sabotage of key automated elements or even the inadvertent failure of one or more systems. Such an attack can occur without forewarning or escalation of other events. "The US no longer has its traditional, geographically-based strategic sanctuary."[6] Current National Information Infrastructures do not provide adequate security to protect systems from break-ins, hacking, or purposeful sabotage from a wartime opponent. The US military and private corporations must work together to ensure that information infrastructures within rail and port facilities that are vital to command and control of military operational deployment are adequately protected from attack.

---

[3] Volpe Center, Summary of the seminar on "Emerging Issues in Transportation Information Infrastructure Security," 21 May 1996 http://www.volpe.dot.gov/resref/archives/series1.html (17 December 1999) 2.

[4] Ibid., 4.

[5] Thomas Andersson and Patrick Hasson, "Why integrated transport?" The Organization for Economic Cooperation and Development Observer. Paris April/May 1998, 34.

[6] Kenneth Minihan, Lieutneant General, USAF, Director NSA. "Statement." U.S. Congress. Senate. Committee on Governmental Affairs. Vulnerabilities of the National Information Infrastructure. Hearings before Committee on Governmental Affairs. 24 June 1998, 2.

This paper will examine the vulnerabilities that are inherent with the implementation of new technologies in the critical infrastructures that the US military will depend upon to deploy large units, specifically rail and port vulnerabilities. First, a definition of Information Warfare will be given. The paper will also address how waging Information Warfare against critical infrastructures such as transportation can affect military deployments. Then, a notional scenario will set the scene for the execution of an operation order to deploy a Mechanized Infantry Division to assess how Information Warfare can be waged to bring the "fog of war" to US ports and delay or deny operational deployment. Finally, recommendations will be given as to how the military and the private sector should work together to secure or "harden" networks that are vulnerable in the transportation infrastructure.

The Problem

Information Warfare is defined by DoD as "actions taken to affect adversary information and information systems while defending one's own information and information systems."[7] However, since this definition is so broad, for the purposes of this paper, Information Warfare will be defined as "nonkinetic, offensive actions taken to achieve information superiority by affecting enemy information-based processes, information systems and computer-based networks."[8] Information Warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-networked systems and often use previously conquered systems to launch their attacks. Information Warfare engagement during an operational deployment will lead to an increased demand

---

[7] Byard Clemmons Q. and Gary D. Brown. "Cyberwarfare: Way, Warriors, and Weapons of Mass Destruction." Military Review, September/October 1999, 35.
[8] Ibid., 35.

for information, while the capacity of the information infrastructure to provide information may decrease.

Military and commercial networks that are the backbone of the US critical infrastructure must be protected from Information Warfare attacks to promote US national interests and ensure strategic and operational stability. Strategic interests that should be defended against Information Warfare include economic interests to support a free market economy and a favorable balance of trade, of which transportation is a major part. Operationally, military interests need to be defended from Information Warfare, so that the US can maintain the ability to sustain a military force that is ready to fight and that can be quickly deployed where needed. Protecting the military capability to deploy is becoming increasingly more difficult as deployment is rapidly becoming more dependent on critical infrastructures, such as transportation, that are vulnerable to Information Warfare. The reality is that the vulnerability of DoD and commercial systems, to offensive Information Warfare attack is largely a self-created problem. Program by program, economic sector by economic sector, the US has based critical functions on inadequately protected computer networks. US commercial systems are increasingly more vulnerable to IW attacks.

In a number of commercial organizations, the trend is to make their systems more open and accessible. This is especially true in intermodal transportation. Computerization touches every aspect of intermodal movements: rating, routing, control of containers, clearance, reporting and all other functions. One such application that is important to both commercial transporters as well as military transporters is Electronic Data Interchange (EDI), an automated reservation system that shares information on

freight shipments. Ironically, this desire for more open systems may bring better worker efficiency and customer benefits, but it also inevitably increases the system's vulnerabilities. Overall, the US has created a target-rich environment and the Information Services industry has sold globally much of the generic technology that can be used to strike these targets.[9]

As Computer systems are increasingly interconnected, it can become easier to reach and target several of them by exploiting a single vulnerable point. Information Warfare is also relatively cheap to wage as compared to conventional warfare, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous. Key technologies designed for completely innocent applications can be used as weapons. For example, software used to test systems can also be used to penetrate systems. Recently a new breed of hacker software that can learn and adapt to the network environment it attacks has become available.[10] This may represent a new threat to commercial systems as well as the military systems that are critical for US military deployments. According to information technology experts, the new programs can change their mode of operation, or their targets, based on external stimulus. Pre-programmed to search for specific types of files common to most networks, such software, once in the system, can target data or files of interest to intruders, even those marked secure or for internal use only.[11]. Therefore, an attacker could easily begin to follow trends in commercial computer systems. If such a program was applied to EDI, the system that US port facilities and rail lines use to track documentation associated with the transport of goods and military

[9] Volpe Center, 4.
[10] Vernon J. Ehlers, "Information Warfare and International Security." The Officer, September 1999, 29.

equipment, an attacker could detect that more military equipment is being transported to and staged at port facilities, and booked for shipment overseas. By merely tracking trends that were spotted by software, a resourceful attacker could predict exactly where and when the US plans to deploy, and launch attacks against information systems to delay a deployment.

Another tool that is available to hackers was developed in Germany, and performs over five thousand checks each minute against a system looking for vulnerabilities.[12] Finally, the threat is spreading to government sponsored Information Warfare. According to James Mulvenon, a defense specialist at Rand Corporation, China is seeking the ability to interfere with Taiwan's command system and ultimately to hack into US military networks that control deployment in the Asian region.[13] One such network could be the Global Transportation Network.

"GTN's vision is to gather the family of transportation customers and providers of lift into a single integrated network that will provide in-transit visibility and the command and control capabilities necessary to support their needs."[14] GTN has integrated current DoD systems, primarily the Defense Transportation System, and commercial automated transportation systems to provide seamless logistics support to the military customer to meet transportation requirements. EDI will provide in-transit visibility of military cargo moving via commercial carrier, which is estimated to be between 60 and 80 percent of all defense transport.[15]

---

[11] Ibid., 30.
[12] Volpe Center, 7.
[13] Ehlers, 28
[14] U.S. Transportation Command, "GTN-Global Transportation Network" http://wwwgtn.satb.af.mil. (20 January 2000) 2
[15] Ibid., 2.

"Many organizations, from both the DoD and commercial industry are responsible for managing their existing and future automated systems and needs. USTRANSCOM is responsible for ensuring those DoD and, to the maximum extent, commercial industry automated transportation systems are developed, integrated, and maintained to support the transportation community as effectively and efficiently as possible."[16]

The Global Transportation Network therefore uses unclassified data sources and interfaces with the Global Command and Control System (GCCS). GCCS will continue to increase in importance as it becomes the system through which CINCS, JTF, and other commanders gain access to more and different information sources. Although GCCS has undergone selected security testing, much remains to be accomplished. For example, security testing to date has focused principally upon Oracle databases and applications evaluation. Other GCCS aspects need thorough security testing; e.g. database applications, message functions, and configuration management. Because the GTN is interconnected with the commercial networks, it is difficult to detect exactly where there is a weak link in the system. Roy Rumsey, an information security expert with Creative Technologies Incorporated indicates that part of the problem lies within NIPERNET.

"Each military base, ship, plan, organization at one time or another may have had a direct connection to the Internet with a backend connection to the NIPERNET. This means there are thousands of points of entry that all need to be secured and managed. A flaw in any one of these exposes the entire NIPERNET to vulnerabilities."[17]

With this in mind it is possible to see how information security is a moving target. John Hamre, Deputy SECDEF recently stated that from January to mid-November 1998 NSA recorded more that 3800 incidents of intrusion attempts against the DoD's unclassified computer systems and networks. Over 100 of these attacks reached root-

[16] Ibid.

level access and many were even able to break down some kinds of service. So, just how vulnerable to attack are the US military and private networks that are necessary for deployment?

In the summer of 1997, a simulation exercise called "Eligible Receiver" was conducted at the Pentagon, ordered by the JCS to test the ability of the nations military and civilian infrastructure to resist a concerted Information Warfare attack. A team of fictional hackers, the Red team, was allowed to use only COTS materiel and information available on the web and they had to act within the US law.

"The simulated attacks focused on three main areas including the national information infrastructure. Hackers found it exceptionally easy to penetrate apparently well-defended systems. Air traffic control systems were taken down, power grids made to fail, oil refineries stopped pumping oil. At the same time, in response to a hypotheical international crisis, the DoD was moving to deploy forces overseas and the logistics network was swinging into action. It proved remarkably easy to disrupt that network by changing orders, and interrupting the logistics flow. The exercise proved that a team of skilled hackers, using standard equipment and publicly available information and playing by the rules, was able to cause a serious degradation to the Pentagon's ability to deploy and to fight. In other words, they demonstrated that an "electronic Pearl Harbor" was possible." [18]

The following section will examine how an Information Warfare attack on rail and port facilities could render the military ineffective in deployment operations.

The Threat

CNN Headline News...This just in. Tensions on the Demilitarized Zone between North and South Korea continue to mount. Intelligence sources report that North Korea is currently making moves to amass forces on the DMZ. Military units in the US are mobilizing in preparations for a deployment to South Korea. In other news, two people are dead, and a half million dollars worth of cargo is destroyed as two trains collided head-on outside of Long Beach Port facilities. A Santa Fe train and a Southern Pacific

---

[17] Roy Rumesy is an information security expert in Washington DC. Rumsey has worked with several government agencies assisting with infosec, including CIA and NRO. Rumsey, Roy. rrumsey@erols.com "Research" 16 January 2000. Office Communication. (16 January 2000)

[18] Ehlers, 32

train were traveling at a high rate of speed when the accident occurred. Southern Pacific, the line that operates the switches on the rail line, claims a problem in the computer program that controls the switches rerouted the Santa Fe train, causing the crash. No word yet as to how long clean up will take, or how it will effect traffic moving into and out of the port.

The Plan

The Port of Long Beach will be used for major deployments in the Pacific.[19] In this scenario, the US military will be using the Port of Long Beach for deployment to the Korean Peninsula to assist the South Koreans in defending against an imminent attack by the North Koreans. The Port of Long Beach must be prepared to grant priority use of Maersk Marine Terminals which includes three berths at one container pier; 15 acres of open storage; about 12,000 square feet of covered storage; and about 300 square feet of office space. The likely requirement for the Port of Long Beach is to deploy a notional mechanized infantry division in six days of reception and throughput. This division must move about 7,800 vehicles and 660 containers. Movement to the port will require 1,055 railcars at the rate of 176 per day. Movement out of the port will require nine fast sealift ships (FSS), and it is assumed three ships will depart every two days. Therefore, three sustained loading operations will be necessary to meet staging and deployment requirements.[20]

The Vulnerabilities

Staging of equipment for a deployment presents a problem. Containers are now shipped from depots to ports either by train or by truck with a tracking number. The tracking number is entered into EDI and GTN, and the tracking number is electronically

---

[19] Fraunfelter Mike Lt. Col. Logistician, Military Command Center, USTRANSCOM, Interview by author, 27 December 1999.

[20] A compilation of information from Burgener, Paul. West Coast Ports for National Defense. Falls Church, VA: Military Traffic Management Command, September 1994. Specific planning requirements in response to a military deployment are outlined in the Port Planning Orders issued by MARAD.

read as it enters the gate at the port. The containerized cargo is then directed to a staging area at the port. A resourceful attacker need only transpose some of the tracking numbers, and containers could be sent to other portions of the port, where they are diverted from the deployment efforts. Lets assume that 73 containers (an entire container cargo for one ship) full of ammunition and spare parts are redirected through a bogus order to an improper staging area, and another 73 containers of the same dimensions arrive on the quay where a US FSS ship is awaiting transloading operations to begin. It is possible that in the commotion of loading operations, the faulty tracking number will be missed by a clerk checking a manifest (if the manifest was not also changed) and the wrong cargo would be loaded onto the vessel, i.e., teddy bears vice bullets. Conversely, the clerk could notice that the tracking numbers do not match the containers, in which case an investigation, followed by a search for the containers would ensue. If the containers were not already loaded onto another vessel that departed, the operation would only be delayed until the containers could be located, moved to the proper staging area and loaded. If the cargo was loaded onto another vessel that sailed, then operations will be delayed until a replacement cargo could be brought in. Under either scenario, it is unlikely that the requirement to deploy three ships every two days will be met.

Berthing of ships is also vulnerable to attack. Berthing orders can easily be switched without detection, sending operations into disarray. While it is true that in this order, berths that are to be used are predetermined, a skillful hacker could change electronic orders directing ships entering the port facility to berths that are not adequate for a vessels needs. If an FSS ship that is used in this scenario were to be rerouted to a berth that had an inadequate depth, the ship might hit bottom and sustain damage, or

conceivably run aground. This would take at least one of the nine necessary ships temporarily out of commission, and delay the required sustained loading operations by at least 33%. Another vessel could be sent to a berth that has an insufficient ramp clearance at low or high tide making it impossible at certain times to load the notional division onto the RORO, causing yet another delay in having to move the vessel. Finally, ships could be sent to a berth that does not have the necessary port services such as water, power, and communications to sustain the vessel. Ships could be sent to berths that do not have the crane capacity to load heavy equipment onto vessels, leading to physical vulnerabilities such as broken or damaged cranes, or worse, a damaged ship and injured personnel from an ensuing accident such as a crane dropping its load onto the deck of a ship. All of these factors could significantly hamper the loading of military cargo onto a vessel denying the sustained loading operations that are necessary to meet the requirements of deployment. If in fact the bogus orders are detected, and a ship is eventually redirected to the proper berth, the attacker was still successful in delaying the loading of the vessel.

The scenario above already demonstrated one of the most devastating impacts that a computer hacker could have on a rail line. By hacking into the rail systems, railcars can be rerouted, causing significant damage and devastation to life and property. Such an incident could tie up a rail line for days, while the wreckage is cleaned up and an investigation is launched. In this scenario, it was not mentioned what kind of cargo was destroyed in the wreck. However, in an extreme case a hacker can follow a shipment from the depot to the port since the information was entered into EDI and GTN. He would therefore know what train military equipment was on, and would be able to

reroute that specific train, leading it into an "accident" that would destroy equipment, hence denying any deployment.

An attacker can also break into the computer system of the port to take down necessary functions such as electrical power grid that runs the computers at the gates, electric rail lines, and cranes, seventeen of which are at the berths that are designated for this notional deployment. While ports have several redundancies in their main computer systems, which can be repaired quickly, it is nevertheless a course of action that should not be overlooked. If taken down for as little as half an hour, port operations will be severely backed up as throughput at the reception gate, rail lines and berths would be significantly hampered.

This brief scenario has shown how computer hackers can cause considerable confusion in a deployment operation. While the consequences of an information attack range from misplaced containers to a loss of life, each incident serves to delay operations. Each delay cascades throughout the entire operation, significantly delaying departure from the US, and effecting operational tempo in the theater that is anticipating the on time arrival of military equipment and troops.

Recommendations

This paper has demonstrated that the cascading effects of attack on critical infrastructures, such as transportation can keep the US from fulfilling one of it's most essential missions, that of deployment. In order to prevent cascading effects of Information Warfare from actually occurring, the US must promote awareness of vulnerabilities, provide deterrence from Information Warfare attackers, and persevere in ensuring security between commercial as well as DoD networks.

Everyone must be made aware of the vulnerabilities that are inherent in the current system. Traditional thinking is that infrastructures, with few exceptions, are stable, reliable, and always available. The nation's rail and port facilities are no exception. Consequently, the DoD's operational and functional planners have not adequately addressed the possibility that key infrastructures such as transportation might not be available to support military operations. Operational and functional planners should begin documenting the extent to which plans for mobilization and deployment are dependent on critical infrastructures and what effect infrastructure disruptions might have on the execution of those plans. Joint Doctrine should address defense against Information Warfare for US systems that are necessary for military operations. Finally, the US government must work with the private sector to convey the importance of security within commercial systems that are vital for operational deployment. Perhaps involving the commercial sector in exercises or wargames would increase awareness of how vulnerable commercial systems are, and the cascading impact of Information Warfare against such vulnerabilities.

Just as the US used deterrence during the cold war to prevent nuclear attacks, the US must deter Information Warfare attacks. This deterrence must include national will expressed in enforceable laws and conduct. Currently, existing laws, particularly international laws, are ambiguous regarding the definition of criminality in and acts of war on information infrastructures. This ambiguity, in conjunction with a lack of clearly designated responsibilities for defense, constrains the development of remedies and limits response options. Specifically, rules of engagement regarding appropriate defensive actions that may be taken must be established upon detection of intrusions into and

attacks against DoD systems and commercial systems that are used for operational planning. In addition, DoD's role in defending commercial systems that are vital to operational planning must be made clear. This should specifically include the exploitation of information on unidentified intruders by intelligence collection, The issue of collecting against US citizens that would participate in this type of activity would have to be addressed. The Government should establish an Information Warfare Defense Center within DoD aimed specifically at collecting intelligence to guard against such attacks, and protecting critical infrastructures with in the National Information Infrastructure. This organization should be granted the authority to conduct "hot pursuit" of intruders in to vital systems. Another deterrent option for the US would be a strict declaratory policy on consequences of an Information Warfare attack against the United States. Finally, an indication of the resiliency of the information infrastructure to survive an attack will also act as a deterrent. Even if the transportation system can be taken down temporarily, it is often difficult to keep systems down for long periods of time. The US information infrastructure has show resiliency in the past and must continue to do so, so that the threat of Information Warfare will quickly erode as soon as administrators begin to react to the attack.

The most immediate need is to provide some form of protection agianst Information Warfare. Because so much of the military's operational deployment needs are met by private sector industries, this protection of systems requires the effective collaboration of both of these groups. Therefore, it is sensible for the military to assist private sector infrastructure organizations to identify information security vulnerabilities and take actions to resolve them before they have a chance to disrupt vital national

security activities. Key infrastructure elements, particularly transportation have historically been major targets during warfare and should be protected through encryption and isolation, access control, and hazard analysis. Data encryption for distributed systems, such as EDI, would make tracking information regarding a certain cargo difficult for computer attackers. Isolation of networks that are used during wartime would be another option to make a hackers job more difficult. Access control on data would ensure that only authorized users can perform specific tasks. Finally, hazard analysis tools that perform safety checks on critical functions should be installed in transportation networks. These tools could monitor unexpected changes in systems that control functions, such as rail switches, where a life may be endangered by a failure. Improving security for systems which are critical to military deployments are necessary for both military and commercial systems, and risks should be managed by these two entities before US national security is at stake.

Conclusions

This paper has shown that the United States has put itself into a position of being vulnerable to Information Warfare attacks against critical infrastructures such as transportation. The United States military relies on military systems as well as commercial systems at rail and port facilities for rapid deployment capability. Because several of the systems that are relied upon do not have adequate security, an Information Warfare attack against these systems can and will deny the military the capability to deploy rapidly, severely hampering operational tempo. Information Warfare attacks against US rail or port facilities could cause so much confusion and the cascading effects could run so deep, that the US could reach culmination prior to even leaving the shore. It

is vital that the US make commercial entities aware of the vulnerabilities, and help to protect those systems where ever possible. Finally, just as the US deterred nuclear warfare by stating that the consequences of such an act would be more costly to the attacker, so must the US deter the Information Warfare attacker by assuring that punishment will be swift, just and costly. The US military cannot afford to have deployment capabilities disrupted, delayed or denied. As the only super power left in the world, the US must be capable of power projection to protect US national interests abroad.

Bibliography

Books

Burgener, Paul. West Coast Ports for National Defense. Falls Church, VA: Military Traffic Management Command, September 1994.

Muller, Gerhardt. Intermodal Freight Transportation. Lansdowne, VA: Eno Transportation Foundation, 1995.

Articles

Andersson, Thomas and Patrick Hasson. "Why integrated transport?" The Organization for Economic Cooperation and Development Observer. Paris; April/May 1998.

Anonymous. "Army Tests Intermodal Surge." Army Logistician, March/April 1998, 45.

Ayers, Robert. "The New Threat: Information Warfare." RUSI Journal, October 1999. 23-27.

Clemmons, Byard Q. and Gary D. Brown. "Cyberwarfare: Way, Warriors, and Weapons of Mass Destruction." Military Review, September/October 1999, 35-45.

Ehlers, Vernon J. "Information Warfare and International Security." The Officer, September 1999, 28-32.

Mattingly, Joseph G. "Intermodal Transportation." Defense Transportation Journal, April 1999, 5.

Ritchie, Robert J. "Seamless Rail, Road, Water, Air?," , December 1999, 45.

Stauffer, Don. "Electronic Warfare: Battles Without Bloodshed." The Futurist, January February 2000, 23-26

US Government Documents

U.S. Department of Defense. "Report of the Defense Science Board Task Force on Information Warfare-Defense" Washington: November 1996

Minihan, Kenneth, Lieutneant General, USAF, Director NSA. "Statement." U.S. Congress. Senate. Committee on Governmental Affairs. Vulnerabilities of the National Information Infrastructure. Hearings before Committee on Governmental Affairs. 24 June 1998.

Robertson, Tony, USAF, CINC USTRANSCOM, "Written Statement." U.S. Congress. House. Armed Services Readiness Subcommitee. Statement of Gen. Tony Robertson. Submitted written statement to the House Armed Services Readiness Subcommitee. 26 October 1999.

Electronic Documents

Lewis, Brian C. "InformationWarfare." http://www.fas.org/irp/eprint/snyder/infowarfare.htm (16 January 2000)

Libicki Martin. "Ghosts in the Machines?" USIA Washington File. 4 Novemeber 1998. http://www.fas.org/irp/news/1998/11/98110403_plt.html (22 January 2000).

Rumsey, Roy. rrumsey@erols.com "Research" 16 January 2000. Office Communication. (16 January 2000)

Tenent, George. "China, others spot U.S. computer weaknesses: CIA." http://www/freerepublic.com (20 January 2000).

U.S. Transportation Command, "GTN-Global Transportation Network" http://wwwgtn.satb.af.mil. (20 January 2000)

Volpe Center. Summary of the seminar on "Emerging Issues in Transportation Information Infrastructure Security." 21 May 1996 http://www.volpe.dot.gov/resref/archives/series1.html (17 December 1999)

Interview

Fraunfelter Mike Lt. Col. Logistician, Military Command Center, USTRANSCOM Interview by author, 27 December 1999.